International Letters of Social and Humanistic Sciences *Online: 2013-09-25*
ISSN: 2300-2697, Vol. 6, pp 41-48
doi:10.18052/www.scipress.com/ILSHS.6.41

Attributed Metagraph Modelling to Design Business Process Security Management

Debiprasad Mukherjee

Sr. Business Analyst., Business Process Management, Cognizant Technology Solutions,
53/1/1 Baksara Road. Howrah – 711110, WB, India

E-mail address: debiprasad.mukherjee@gmail.com

ABSTRACT

Cross organizational process flow is having increasing importance as organizational focus is on offshoring & outsourcing to develop complex business processes. Utilizing the development of telecommunications frameworks, IT systems are fundamental to collaborating and distributing business processes for both internal as well as external business units. But, this increased dependency exists in an ecosystem of increasing threats to information security along with market sensitivity and regulatory power. Based on recent process flow studies, we explore application of attributed metagraph representation to evaluate process security. Utilizing examples of both risk-analysis and impact-mitigation, we reveal the effectiveness of attributed metagraph for business process analysis. Metagraph-based model helps in analysis of as-is processes as well as offers normative direction for process remodelling.

***Keywords*:** business processes; telecommunications; information security; metagraph

1. INTRODUCTION

As discussed, organizations are gradually moving towards offshoring and outsourcing locally and worldwide, in order to execute distributed processes across organization. Having already aligned production-based work with information-based work, the types of information-intensive processes are now moving to larger and more complex processes (Kriplani 2006). Information Technology (IT) is the most important factor of the present ecosystem that is required to coordinate these dispersed processes.

As the dependency on distributed systems is growing, the privacy & security of information resources is under threat. Market inspection and regulations are adding major consequence for organizations which fail to prevent disclosure of secured information, especially across organizations. Concerns about protecting company and employee information are preventing many organizations from further exploiting the probable benefits of offshoring and outsourcing (Richardson 2006). Hence, when analyzing the design of business processes in an organization, security and protection are the key focus areas.

Security has always lagged general IT systems development methods (Baskerville 1993); this is an absolute truth in business process designing also. As the importance of security changes from static risks which can be mitigated by constant safeguards to unpredictable random risk requiring emergent mitigation plan (Baskerville 2005), tools and techniques for swiftly identifying and analyzing process security are required.

To handle this problem in business process analysis and modelling, we show that an attributed metagraph representation of cross-organizational business processes can be successful for security scrutiny. While both petri nets and metagraphs can be used for process analysis & design, this research emphasizes on cross-organizational (Basu 2005) and attribute-based (Basu and Blanning 2001) representations using examples of risk & impact analysis.

2. ATTRIBUTED METAGRAPHS

Graph-theoretic approach of analyzing process flows and designing process maps provides insight into typical process modelling problems and helps in designing effective process flows. Modelling of process flows as metagraphs has been designed to provide a concrete basis for formal analysis of business processes and workflows.

Metagraph is a graphical hierarchical data structure where every node is a specific set having one or more elements. It has all the properties of a typical graph. In a metagraph, there is set-to-set mapping in place of node-to-node as in a conventional graphical structure. In a Metagraph as data structures, data will be stored inside the computer memory either in the form of Adjacency matrix or in Adjacency list so that it can be used efficiently.

Fuzzy Metagraph and Vague Metagraph are emerging techniques used in the design of many information processing systems like transaction processing systems, Decision Support Systems (DSS), and workflow Systems.

Like traditional graphs, metagraphs also having a set of edges connecting a set of nodes. Edges of the metagraph are directed (just like digraphs) and nodes contain sets of elements (like hypergraphs). The combination of directional-edges and set-based-nodes supports various vital systems of metagraphs like modelling of decision support systems (Basu and Blanning 1994), study of assumptions in model bases (Basu and Blanning 1998), formal analysis of process flow (Basu and Blanning 2000, Basu and Blanning 2001), and cross organizational process coordination (Basu 2005). Importance of metagraph representation is it supports not only for visual modelling but also helps in algebraic analysis.

The inclusion of algebraic operators is absolutely necessary for tool-based analysis of complex processes and systems. A relatively new concept, “the range of rigorous tools available for validation, verification, and performance analysis are limited” (Barkataki 2003, p. 2). Our intension is to contribute to the development of precise tools for analysis by emphasising on leveraging metagraphs to present cross-organizational business processes. For this kind of representation, the nodes of the metagraph stand for set of resources necessary for a process; the edges symbolize the business processes which utilize or change source resources to generate target resources. Previous researches on attributed-metagraphs (Basu and Blanning 2001) has labelled edges with qualitative or quantitative attributes such as time-to-process and used metagraph operations for scheduling.

This study extends attributed-metagraphs by adding element attributes; specifically, we use the example of elements which may or may not hold secured data. Say for example, secured information could be patient health information with legal regulations. Unlike previous researches on attributed-metagraphs, attribute like “secure” is inherent in an element of a metagraph rather than an edge (process).

Definition: An element attributed metagraph is a metagraph $G = (X_m \cup X_{m'}, S)$ generated from set $X = \{x_l, 1\ldots L\}$ of elements and set $S = \{e_k, 1\ldots K\}$ of edges in which the set X_m contains elements with attribute m,
X_{m^-} contains elements without attribute m, and $X_m \cap X_{m^-} = \Phi$. (m^- denotes m bar)

With the help of element attributed-metagraph, an edge attributed-metagraph (Basu and Blanning 2001) can be developed by designing an attributed-edge as an edge, e_k, with minimum one source element $x_l \in X_m$

Having created a connection between element-attributed metagraphs and edge-attributed metagraphs, the rest of the paper utilizes operations defined for edge-attributed metagraphs to analyze & design the process security.

In the next section, this research presents the analysis of process risks through recognition of the exposure of secured elements and inclusion of layers to minimize exposure. Then, we leveraged metagraphs to analyze the effect of process failure by identification of redundant, functionally comparable processes and quantification of the differences of unnecessary and redundant processes.

3. ANALYZING RISK

A significant aspect of security analysis & design is risk assessment (Baskerville 1993). We concentrate on two types of risk analysis— classification of exposure of secured data and inclusion of layering to minimize exposure. For risk analysis and design, consider the metagraph presentation of two business processes (Figure.1) that depicts patient information to generate a directory of patients (edge *e2*) and to generate invoice (edge *e4*).

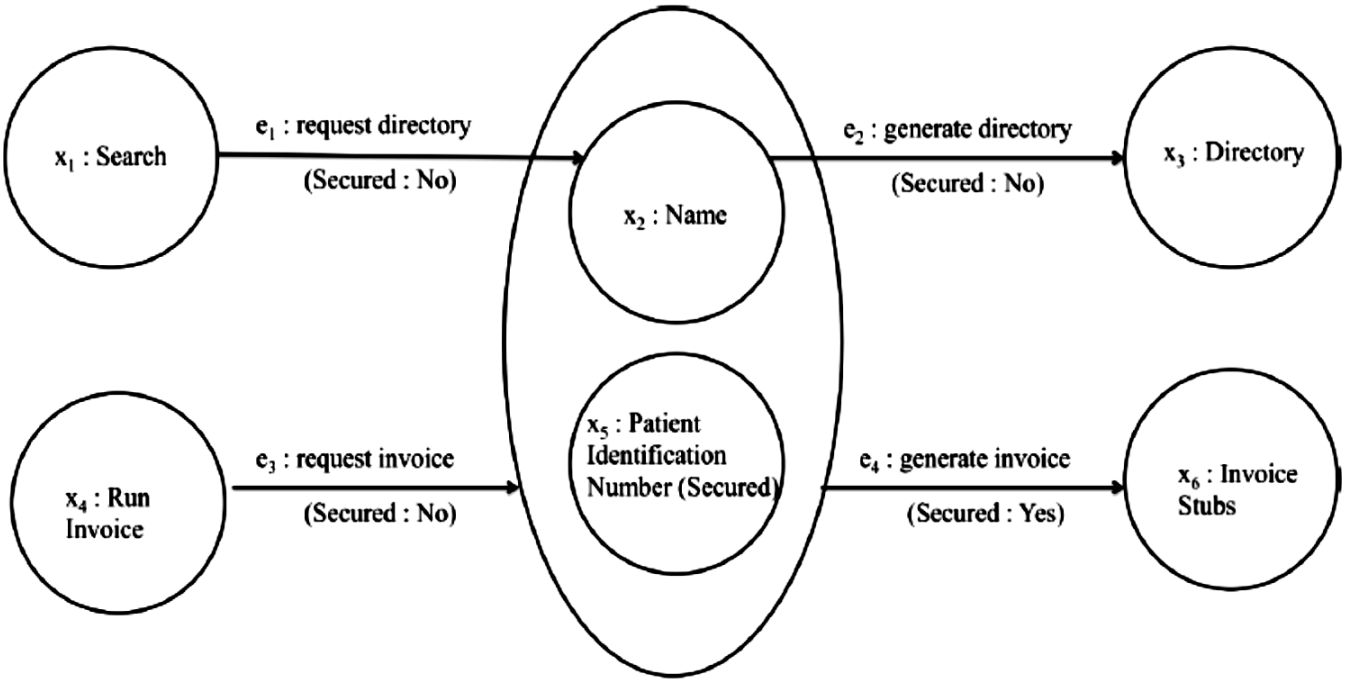

Figure 1. Metagraph of Secured-Information containing processes.

Edge *e2* connects patient name (vertex *x2*) to the patient directory (vertex *x3*) and edge *e4* links both patient name (vertex *x2*) and patient identification number (vertex *x5*) to the patient invoice stub (vertex *x6*). Other edges (*e1* and *e3*) and vertices (*x1* and *x3*) initiate the processes.

Each of the edges has the value of Yes/No for the Secured-attribute depending on whether the process (edge) involves secure information. Process *e2* represents search functionality on a

public website which takes a partial name and returns list of corresponding patient names and do not contain secured information.

Process e_4 represents producing patient invoice and, since it has a secured-source element (patient identification number), has the value of 'Yes' for the Secured-attribute.

3. 1. Identifying Exposure

Consideration of process e_2 only would not specify a security problem: it neither contains nor generates secured information. In the example, the data set which has patient name also contains the patient identification number. Hence, a compromise of edge e_2 could be a cause of data security threat. As an example, if the website user query request is not getting verified, a data security attacker could have entered unanticipated structured query language (SQL) commands. Known as SQL injection, this method threatens other data elements within the data set.

By adding attribute, the protected processes in visual representation can be quickly recognized for small examples. For real examples with different complex business processes, exposure is not as easy to recognize visually. Instead, by analysing the shortest available path from a set having a secured element to a process, leveraging prior definitions of length and path (Basu and Blanning 2000), the exposure of a secured element to a specific process can be quantified. Moreover, closure of the adjacency matrix for a metagraph (Basu and Blanning 1994) can help in identifying algebraically the length of all paths from secured elements to other elements. The path length to a secured element is of great importance when a target element is external to the organization or an edge in the path is outsourced.

Previously, different approaches were proposed for increasing security. Synthesis of processes (Basu and Blanning 2003) can hide secured elements within a business process boundary. Otherwise, a projection of metagraph can also hide secured elements (Basu and Blanning 1998). However, while helpful in restricting secured information from a user, both synthesis and projection impair the ability of an analyst to decide exposure of secured data. By focussing on secured elements rather than hiding them, this research supports quick analysis of business process security, mainly in response to unpredicted risk (Baskerville 2005).

3. 2. Layering

The theory of defence identifies that systems and security will never be perfect at all. Multi-layers of security are required so that even if there is failure in one layer, data can still be protected. Once the path lengths from externally accessible elements have been recognized, additional processes (edges) can be involved to increase the minimum path length.

In Figure 2, the edge e_5 is depicted to increase the path length from secured element x_5 to the generated directory. Leveraging the adjacency matrix, the impact of the new process can be made quantifiable.

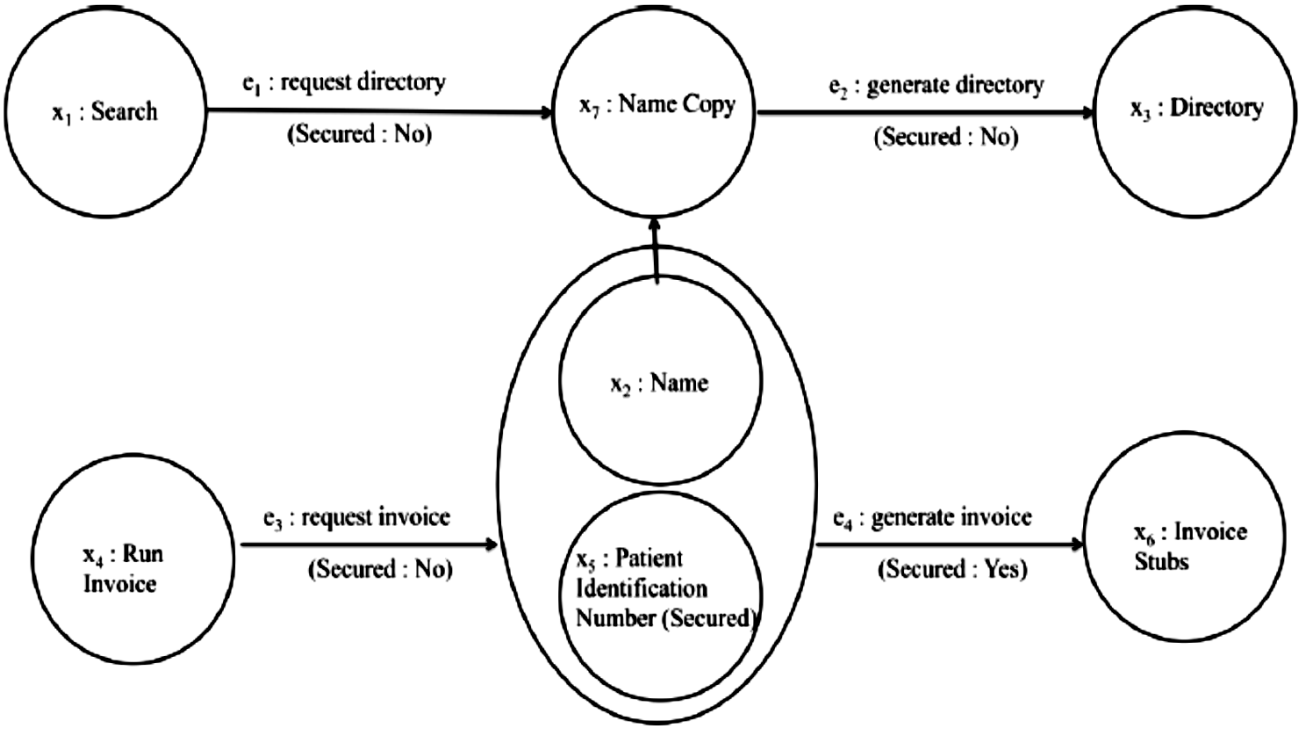

Figure 2. Metagraph of Processes with Layer.

4. ANALYZING IMPACT

Another vital factor of security is to analyze the business impact of failure of a process. Processes may fail for different reasons internal to the process (for example, disruption of a required information system) or external to the process (for example, natural disaster in the geographic location where the process is performed).

For impact analysis, we have considered the metagraph modelling of a business process (Figure 3) that generates patient invoices by first matching invoices with purchase orders (edge e_{2i}) and then paying invoices (edge e_{3i}). Edge e_{2i} connects both the received invoice (element x_2) and the original purchase order (element x_3) resulting in a matched invoice (vertex x_4). Edge e_{3k} generates a check (element x_5) from matched invoice (element x_4).

The other edge (e_1) and element (x_1) starts the process. Edges e_{2i} and e_{3j} have vectors of related attributes ($\boldsymbol{Y_i}$ and $\boldsymbol{Z_j}$ respectively) which denotes, for example, the geographic location where the process is performed.

4. 1. Redundancy

One technique for insulating the overall process framework against disruption of one process is by redundancy. Redundancy can be considered a form of process indistinctness to be removed (Basu and Blanning 2003), it can also offer the organization a way to recover from the failure of an edge; metagraph modelling can identify equivalent business processes.

Definition: With exclusive names of elements (Bhargava, et al. 1991), two edges, e_m and e_n, are *operationally equivalent* if and only if, given the source vertices of e_m ($v_{s,m}$), the source vertices of e_n ($v_{s,n}$), the target vertices of e_m ($v_{t,m}$), the target vertices of e_n ($v_{t,n}$): $v_{s,m} = v_{s,n}$, and $v_{t,m} = v_{t,n}$

To make every set of vertices equal, all the data elements within the vertices must be same and should refer to the same data elements requiring that distinct elements be distinguishable (Bhargava, et al. 1991).

As an example, if checks are produced by two different processes in different geographic areas, then distinctly named checks must be equivalent. Otherwise, if one check is calculated with one country's withholding and another with some other country's withholding, then the two checks need distinct names, would not be equivalent and the business processes that generated them, hence, should not be operationally equivalent.

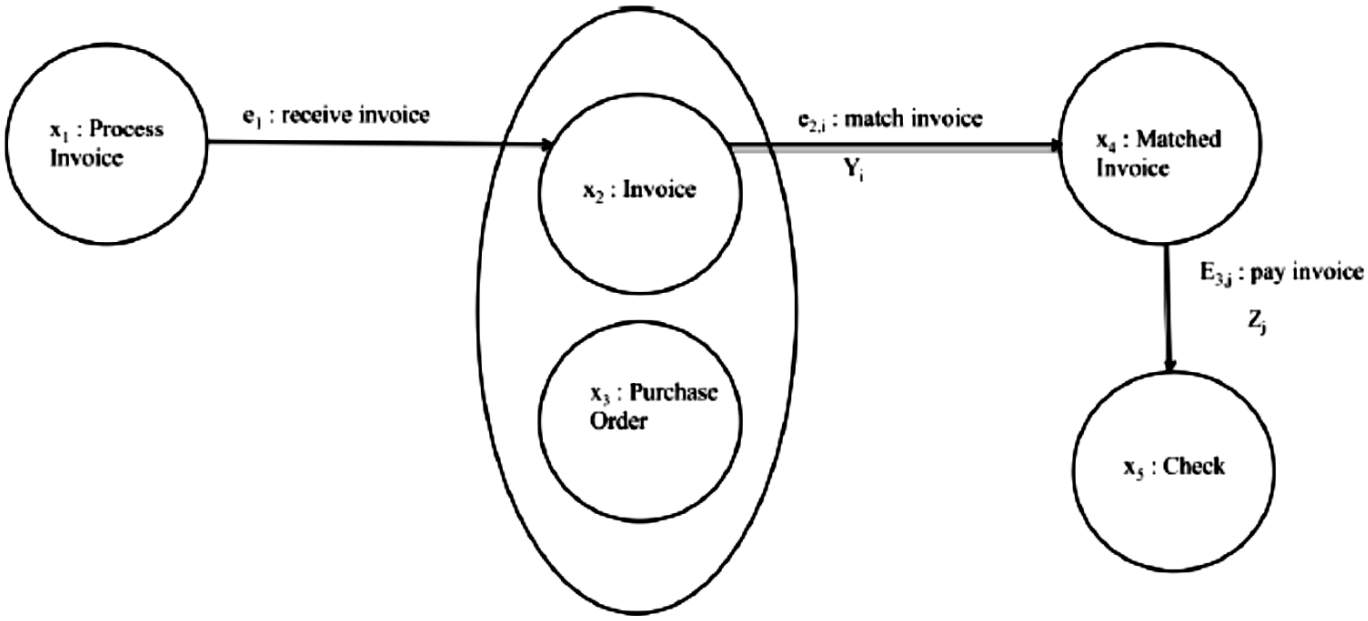

Figure 3. Metagraph Modelling of Redundant Simple Processes.

4. 2. Diversity

Absolutely redundant business processes, however, would not be desirable. To offer redundancy against failure, minimum one attribute of the functionally equivalent processes must change. As an example, if the vector $\boldsymbol{Y_i}$ has an attribute, l, representing the geographic location where the process is done, then $\boldsymbol{Y_{i,l}}$ must not equal $\boldsymbol{Y_{\bar{i},l}}$ for a operationally equivalent process to offer redundancy for a disruption in geographic location.

As the number of attributes on every edge is the same, a simple measure of the diversity offered by an operationally equivalent process would be the Hamming Distance (Hamming 1950). Given two operationally equivalent processes, the distance is the no. of substitutions required to design the string presentations of the vector of attributes of every process the same. This distance defines the diversity in the processes. Moreover, the definition of operationally

equivalent processes can be used in identifying processes which can be leveraged for structural analysis which is not present in general workflow management systems and of particular significance when some processes are part of a cross-organizational process flow (Basu and Kumar 2002).

Table 1. Security Design and Related Metagraph Modelling.

Security Theory	Metagraph Methods	Reviewed Literature
Exposure of secured data	Determination of paths to secured data	Adjacency matrix (Basu and Blanning 1994)
Layering to provide defence	Calculation of path lengths to secured information	Adjacency matrix (Basu and Blanning 1994)
Managing redundant processes	Identification of operationally similar processes	Redundancy (Basu and Blanning 2003)
Diversification of redundant processes	Calculation of diversity of operationally similar processes	Metric of diversity (Hamming 1950)

5. CONCLUSION

Determining the risks and analyzing impacts of security compromise is a vital factor of business process engineering. Using attributed metagraphs modelling, this paper has demonstrated an approach for business process analysis and design. In spite of offering an end-to-end solution for the complex problem of business process security, preliminary analysis determines major opportunities for further analysis such as managing security attributes through synthesis and decomposition (Basu and Blanning 2003).

Though the metagraph modelling is helpful for quantifying exposure of secured data elements, identifying different secured information elements, enumerating operationally equivalent business processes, and offering a metric of diversity, the desirability of the layering or diversity depends on the objectives of the business process design.

Diversity provides redundancy; this may also need the duplication of secure information elements. However, by involving the theoretical development of process analysis methodology, we add tools to help in process improvement, specifically in an intra-organization context that can handle security concerns and react quickly to changes in the security ecosystem.

Reference

[1] Basu, Amit, "*A Metagraph View-Based Approach to Multi-firm Process coordination*", Proceedings of the CAiSE'05 Forum, Porto, Portugal, 2005,

[2] Basu, Amit, Robert Blanning, *Management Science* 44 (7) (1998) 982-995.

[3] Baskerville Richard, *Journal of Information System Security* 1(1) (2005) 23-50.

[4] Basu Amit, Robert Blanning, *Management Science* 40(12) (1994) 1579-1600.

[5] Richardson Karen, *Keeping Accounting Close to Home---Firms Shun Outsourcers as Sarbanes-Oxley Fears Outweigh Any Cost Savings*, The Wall Street Journal, 19 May, 2006, C3.

[6] Ransbotham Sam, Mitra Sabyasachi, *Analyzing Business Process Security using Attributed Metagraphs*, 16th Annual Workshop on Information Technologies & Systems (WITS) Paper

[7] Basu Amit, Robert W. Blanning, *Information Systems Research* 11(1) (2000) 17-36.

[8] Barkataki Sharad, *Mapping Petri Nets and Metagraphs: A Step Towards Inter-Organizational Workflows*, Proceedings of the 9th Americas Conference on Information Systems, 2003

[9] Basu Amit, Robert W. Blanning, *Workflow Analysis using Attributed Metagraphs*, Proceedings of the 34th Hawaii International Conference on System Sciences, Maui, 2001,

[10] Basu Amit, Robert W. Blanning, *Information Systems Research* 14(4) (2003) 337-355.

[11] Bhargava Hermant K., Steven O. Kimbrough, Ramayya Krishnan, *ORSA Journal on Computing* 3(2) (1991) 107-120.

[12] Basu Amit, Akhil Kumar, *Information Systems Research* 13(1) (2002) 1-14.

[13] Kriplani Manjeet, *BusinessWeek* 3996(7) (2006) 40.

[14] Van der Aalst W. M. P., *The Journal of Circuits, Systems and Computers* 8(1) (1998) 21-66.

[15] *Federal Bureau of Investigation*, IC3 2005 Internet Crime Report, 2005, 1-27.

[16] Hamming Richard W., *Bell System Technical Journal* 29(2) (1950) 147-160.

[17] http://www.computer.org/csdl/proceedings/iccsit/2008/3308/00/3308a729-abs.html

[18] http://www.ijcaonline.org/archives/volume56/number6/8893-2910

(Received 10 June 2013; accepted 16 June 2013)